Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of the Claims:

1. (Currently amended) Apparatus operated by a computer service provider and providing one or more computer services for a plurality of customers of the computer service provider, the apparatus comprising:

a real computer, operated by a computer service provider and coupled to a real network, on which is set up at the request of each of ~~said customers~~a plurality of customers of the computer service provider at least one virtual machine for each of said customers~~,~~;

wherein said at least one virtual machine for each of said customers is configured to provide one or more computer services over the real network for each respective customer; and

wherein said at least one virtual machine for each of said customers ~~having~~ comprises a specification specified by and configurable by the respective customer, and ~~having~~ further comprises a separate operating system running thereon.

2. (Original) Apparatus according to claim 1, wherein plural virtual machines are set up within the real computer for at least one of said customers.

3. (Original) Apparatus according to claim 1, wherein the or each virtual machine for at least one of said customers is connected to a virtual network set up for said at least one customer within the real computer.

4. (Original) Apparatus according to claim 3, comprising a virtual intrusion detection device for detecting an attack on the virtual network.

5. (Original) Apparatus according to claim 1, wherein at least one virtual machine is connected to a virtual firewall that is connectable to an external network to which customers and/or other users can connect such that access to said at least one virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

6. (Original) Apparatus according to claim 1, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connectable to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

7. (Original) Apparatus according to claim 6, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connectable to an external network.

8. (Original) Apparatus according to claim 7, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

9. (Original) Apparatus according to claim 5, wherein the or at least one of the virtual firewalls is implemented by a virtual machine on the real computer, said virtual firewall virtual machine running firewall software.

10. (Original) Apparatus according to claim 1, comprising a plurality of real data storage devices and at least one virtual storage subsystem that is configured to allow said real data storage devices to emulate one or more virtual storage devices.

11. (Original) Apparatus according to claim 10, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

12. (Original) Apparatus according to claim 10, comprising a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

13. (Original) Apparatus according to claim 1, wherein the apparatus is configurable to provide at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

14. (Original) Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

15. (Original) Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

16. (Original) Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

17. (Original) Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

18. (Original) Apparatus according claim 1, wherein the real computer comprises plural physical computers.

19. (Original) In combination, a first apparatus according to claim 1 and a second apparatus that is substantially identical to said first apparatus, the first and second apparatus being connected by a communications channel so that the second apparatus can provide for redundancy of the first apparatus thereby to provide for disaster recovery if the first apparatus fails.

20. (Currently amended) A method of providing one or more computer services for a plurality of customers of a computer service provider, the method comprising the steps of:

a service provider setting up on a real computer, at the request of each of said customers, at least one virtual machine for each of said customers of the computer service provider whereby each virtual machine for each of said customers is configured to provide one or more computer services over a real network for each respective customer~~, said at least one virtual machine for each of said customers having~~ ;

the real computer accepting specification and configuration information for the virtual machines from each of said customers whereby the~~a~~ specification of each of the virtual machines is specified by and configurable by the respective

customer ~~and having~~, each virtual machine comprising a separate operating system running thereon.

21. (Original) A method according to claim 20, comprising the step of setting up plural virtual machines within the real computer for at least one of said customers.

22. (Original) A method according to claim 20, comprising the steps of setting up a virtual network for at least one of said customers within the real computer, and connecting the or each virtual machine for said at least one customer to said virtual network.

23. (Original) A method according to claim 22, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

24. (Original) A method according to claim 20, comprising the steps of connecting at least one virtual machine to a virtual firewall, and connecting the or each virtual firewall to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

25. (Original) A method according to claim 20, comprising the step of connecting the or each virtual machine for a particular customer to a virtual firewall that is dedicated to that customer's virtual machine or machines, and connecting each virtual firewall to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

26. (Original) A method according to claim 25, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

27. (Original) A method according to claim 26, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

28. (Original) A method according to claim 20, comprising the step of configuring at least one virtual storage subsystem to allow multiple real data storage devices to emulate one or more virtual storage devices.

29. (Original) A method according to claim 28, comprising the step of configuring the at least one virtual storage subsystem to emulate at least one respective virtual storage device for each customer.

30. (Original) A method according to claim 28, comprising the step of using a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

31. (Original) A method according to claim 20, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high

performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

32. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

33. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

34. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

35. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

36. (Original) A method according to claim 20, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

37. (Currently amended) A method of operating a real computer on behalf of ~~plural~~ a plurality of customers of an operator of the real computer, the method comprising the steps of:

operating ~~plural~~ a plurality of virtual machines on the real computer so as to provide respective computer services for the respective customers over a real network;[[,]] and

receiving at each of said plural virtual machines ~~having~~ a specification specified by and configurable by a respective one of the customers of the operator of the real computer in accordance with a computer service to be provided by the virtual machine on behalf of that customer**[[,]]**;

wherein each of said virtual machines ~~having~~ comprises a separate operating system running thereon ~~so as to provide respective computer services to the respective customers~~.

38. (Original) A method according to claim 37, comprising the step of operating plural virtual machines within the real computer for at least one of said customers.

39. (Original) A method according to claim 37, comprising the step of operating a virtual network for at least one of said customers within the real computer, the or each virtual machine for said at least one customer being connected to said virtual network.

40. (Original) A method according to claim 39, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

41. (Original) A method according to claim 37, wherein at least one virtual machine is connected to a virtual firewall, the or each virtual firewall being connected to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

42. (Original) A method according to claim 37, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connected to an external network to which each of said customers and/or

other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

43. (Original) A method according to claim 42, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

44. (Original) A method according to claim 43, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

45. (Original) A method according to claim 37, wherein at least one virtual storage subsystem is provided and configured to allow multiple real data storage devices to emulate one or more virtual storage devices.

46. (Original) A method according to claim 45, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

47. (Original) A method according to claim 45, wherein a detection device is used for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

48. (Original) A method according to claim 37, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data

warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

49. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

50. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

51. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

52. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

53. (Previously presented) A method according to claim 37, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

54. (Currently amended) A method of providing for a plurality of customers of an operator of a real computer one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting

services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services; the method comprising the steps of:

said operator setting up on ~~a~~ said real computer at the request of each of said customers at least one virtual machine for each of said customers of the operator to provide one or more computer services for each of said customers over a real network~~,~~; and

receiving at said at least one virtual machine for each of said customers ~~having~~ a specification determined in accordance with the computer service or services requested by said customer and ~~being~~ configurable by said customer, said at least one virtual machine having a separate operating system running thereon.

55. (Original) A method according to claim 54, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

56. (Previously presented) Apparatus according to claim 1, wherein at least one of said virtual machines provides at least a virtual central processor unit.

57. (Previously presented) Apparatus according to claim 1, wherein at least one of said virtual machines is created using a virtual machine abstraction program.

58. (Previously presented) Apparatus according to claim 1, wherein at least one of said virtual machines is created using machine simulation/emulation software.

59. (Previously presented) A method according to claim 20, wherein at least one of said virtual machines provides at least a virtual central processor unit.

60. (Previously presented) A method according to claim 20, wherein at least one of said virtual machines is created using a virtual machine abstraction program.

61. (Previously presented) A method according to claim 20, wherein at least one of said virtual machines is created using machine simulation/emulation software.

62. (Previously presented) A method according to claim 37, wherein at least one of said virtual machines provides at least a virtual central processor unit.

63. (Previously presented) A method according to claim 37, wherein at least one of said virtual machines is created using a virtual machine abstraction program.

64. (Previously presented) A method according to claim 37, wherein at least one of said virtual machines is created using machine simulation/emulation software.

65. (New) Apparatus according to claim 1, wherein the one or more computer services for the respective customers are provided over a virtual network which is implemented over said real network.

66. (New) Apparatus according to claim 1, wherein the real computer is arranged such that the specification of said at least one virtual machine for each of said customers is specified by and configurable by the respective customer over said real network or another real network.

67. (New) Apparatus according to claim 66, wherein the real computer is arranged such that the specification of said at least one virtual machine for each of said customers is specified by and configurable by the respective customer over a virtual network which is implemented on said real network or said another real network.

68. (New) Apparatus according to claim 1, further comprising a system configurator program that accepts said specification from each of said customers, said configurator program being operable to modify, based on said specification, the configuration of said at least one virtual machine.

69. (New) A method according to claim 20, wherein said real computer accepting said specification comprises accepting said specification over said real network or another real network.

70. (New) A method according to claim 69, wherein said real computer accepting said specification comprises accepting said specification over a virtual network which is implemented over said real network or said another real network.

71. (New) A method according to claim 37, wherein receiving at each of said plural virtual machines said specification comprises receiving said specification over said real network or another real network.

72. (New) A method according to claim 71, wherein receiving at each of said plural virtual machines said specification comprises receiving said specification over a virtual network which is implemented over said real network or said another real network.

73. (New) A method according to claim 54, wherein receiving at said at least one virtual machine for each of said customers a specification comprises receiving said specification over said real network or another real network.

74. (New) A method according to claim 73, wherein receiving at said at least one virtual machine for each of said customers a specification comprises receiving said specification over a virtual network which is implemented over said real network or said another real network.